



Atty Docket No. 4860.P2436

Patent

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re Application of: ) Examiner: Tran, Tongoc  
 )  
Vogel, J. Leslie III ) Art Unit: 2134  
 )  
Application No. 09/659,864 ) Confirmation No.: 5866  
 )  
Filed: September 12, 2000 )  
 )  
For: USER CONTROL OF A )  
SECURE WIRELESS )  
COMPUTING NETWORK )  
 )

Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

07/24/2006 BABRAHAI 00000008 09659864  
01 FC:1402

500.00 qp

**APPEAL BRIEF UNDER 37 C.F.R. § 41.37**

This is an appeal to the Board of Patent Appeals and Interferences from the decision of the Examiner of Group 2134, dated February 17, 2006, in which claims 1-51 in the above-identified application were finally rejected. This Appeal Brief is hereby submitted pursuant to 37 C.F.R. § 41.37(a).

**I. REAL PARTY IN INTEREST**

The real party in interest is the assignee of the full interest in the invention, Apple Computer, Inc., Cupertino, CA.

**II. RELATED APPEALS AND INTERFERENCES**

To the best of Appellant's knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision in the instant appeal.

### **III. STATUS OF THE CLAIMS**

Claims 1-51 are pending in the application and were rejected in a final Office Action mailed February 17, 2006. Claims 1-51 are the subject of this appeal. A copy of Claims 1-51 as they stand on appeal are set forth in the Claims Appendix.

### **IV. STATUS OF AMENDMENTS**

No amendments to the claims have been made after receipt of the final Office Action on February 17, 2006.

### **V. SUMMARY OF CLAIMED SUBJECT MATTER**

Appellant's invention as claimed in claims 1-51 is a wireless communication network. Claims 1-15, 36-41 and 46-51 claim an access point and a station operating together (Specification: page 10, line 14 through page 14, line 10 and Figure 2). Claims 16-20 and 26-30 claim one embodiment of a station (Specification: page 15, line 6 through page 16, line 2, page 16, line 18 through page 18, line 9, and Figures 3A and 3B). Claims 21-25 and 31-35 claim one embodiment of an access point (Specification: page 16, line 3 through page 18, line 9, and Figures 4A and 4B). Claims 42-45 claim a data structure for messages exchanged between an access point and a station (page 19, line 9 through page 21, line 7, and Figures 2 and 5).

A particular security algorithm claimed in claims 4, 8, 23 and 28 is described on page 18, lines 1-7 in conjunction with formulas 2-5 also shown on those pages.

Claims 46-51 are claims under 35 U.S.C. § 112, sixth paragraph, and the corresponding structures are station 201 and access point 203 of Figure 2 as described on page 10, line 14 through page 14, line 10.

### **VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

- I. Claims 1, 16, 21, 26, 31, 36, 42 and 46 stand rejected under 35 U.S.C. § 112, first paragraph for lack of written description.

- II. Claims 1, 16, 21, 26, 31, 36, 42 and 46 stand rejected under 35 U.S.C. § 102(a) over Patiyoot, et al. (“Technique for authentication protocols and key distribution on wireless ATM networks”, ACM SIGOPS Operating System Review, Volume 32, Issue 4, October 1998).
- III. Claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, 40-48 and 50-51 stand rejected under 35 U.S.C. § 103(a) over Lewis, U.S. Patent No. 6,526,506, in view of Quick Jr., U.S. Patent No. 6,178,506.
- IV. Claims 4-8, 18, 23, 28, 33, 39, and 49 are rejected under 35 U.S.C. 103(a) over Lewis and Quick in view of Schneier (“Applied Cryptography, Second Edition, Protocols, Algorithms, and Source Code in C”, John Wiley & Sons, Inc., 1996).

## VII. ARGUMENTS

- I. Claims 1, 16, 21, 26, 31, 36, 42 and 46 are supported by the Specification under with 35 U.S.C. § 112, first paragraph.

Claims 1, 16, 21, 26, 31, 36, 42 and 46 stand or fall together. Claim 1 is the representative claim with respect to this § 112 rejection. Claim 1 claims a method of establishing secure wireless communications channel between an access point and a station, where the channel is encrypted with a channel key. The station requests a security preference from the access point. In response, the access points sends the security preference, which is one of a set of authentication protocols supported by the access point.

The Examiner asserts that Appellant’s Specification does not disclose more than one authentication protocol, i.e., security preference. Appellant respectfully directs the Board’s attention to page 10, line 20 through page 11 of Appellant’s Specification that sets forth one example of a security preference as being "shared key." Other types of authentication for wireless networks, such as "open system," may be the security preference for a particular network as disclosed on line 7 and page 19, lines 1-5 of Appellant’s Specification. Appellant respectfully submits that "open system" and "shared key" are well-known authentication protocols in the wireless networking art. In

support of Appellant's assertion, Appellant is submitting, in the attached Evidence Appendix, the section 8.1f IEEE 802.11 standard, which states that both "open system" and "shared key" are authentication services and further specifies the particular message frames that form the protocols for the two authentication services.

Furthermore, Appellant specifically pointed to page 19, lines 1-5 of the Specification as supporting the claim amendments in the RCE mailed November 28, 2005. In the final Office Action mailed February 17, 2006, the Examiner did not even address Appellant's statement that the amendments were supported by the cited section. Thus, the Examiner has not established a proper *prima facie* case under § 112, first paragraphs, which requires reasons as to why someone of skill in the art would not have recognized that the inventor was in possession of the claimed invention by reading Appellant's Specification.

Because claim 1 is supported by the Specification, Appellant respectfully submits that claims 1, 16, 21, 26, 31, 36, 42 and 46 satisfy the written description requirement of 35 U.S.C. § 112, first paragraph.

II. Claims 1, 16, 21, 26, 31, 36, 42 and 46 are patentable under 35 U.S.C. § 102(a) over Patiyoot.

Claims 1, 16, 21, 26, 31, 36, 42 and 46 stand or fall together. Claim 1 is the representative claim with respect to this § 102(a) rejection.

Patiyoot discloses using a public-private key pair authentication protocol to authenticate a wireless ATM terminal (WAT) to a wireless ATM server (WAS). Patiyoot discloses that the WAS only supports a single authentication protocol.

Thus, Patiyoot does not teach or suggest an access point sends a security preference that is one of a set of authentication protocols supported by the access point as claimed in claim 1.

Because Patiyoot does not teach or suggest Appellant's invention as claimed in claim 1, Appellant respectfully submits that claims 1, 16, 21, 26, 31, 36, 42 and 46 are patentable under 35 U.S.C. § 102(a) over Patiyoot.

III. Claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, 40-48 and 50-51 are patentable under 35 U.S.C. § 103(a) over the combination of Lewis and Quick.

Lewis discloses a multi-tiered encryption scheme for a wireless network. The first level of encryption is employed between a mobile device and access points on the network. The second level of encryption is employed between the mobile device and a key distribution server. When a mobile device wants to connect to an access point, the mobile device requests the current network encryption key from the key distribution server. The request and the response containing the network encryption key are encrypted with a master key. The access point can also send a new network encryption key to connected mobile devices in response to the key distribution server changing the network encryption key. The access point encrypts the new network encryption key with the old network encryption key. Thus, Lewis discloses an access point that uses a single authentication protocol, i.e., the shared network encryption key.

Quick discloses a subscription service that is portable among different mobile devices. A mobile device generates a public/private key pair from the user's subscription identifier and password. The public key is encrypted with the password. All or part of the unencrypted identifier and the encrypted public key are sent to a server that is local to the mobile device's current location. The local server uses the unencrypted identifier to determine the user's home server and sends the encrypted public key to the home server for decryption. The mobile device is authentic if the decrypted public key matches the public key of the user stored on the home server. Further communication establishes the authentication of the home server to the mobile device. Once both ends of the link are authenticated, credentials can be passed to the mobile device to allow it to register with the local server and obtain an authentication key for the local server. Thus, Quick discloses that the home server and the local server each use a single authentication protocol: the home server shares a public/private key pair with the mobile device while the local server shared an authentication key with the mobile device.

A. **Claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, 40-42, 46-48 and 50-51**

Claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, 40-42, 46-48 and 50-51 stand or fall together. Claim 1 is the representative claim for this § 103(a) rejection.

Appellant claims an access point that supports a set of authentication protocols. As argued above, both Lewis and Quick's inventions support only a single authentication protocol for an access point.

Appellant also claims generating authentication information using a key. The Examiner asserts that Lewis' registration information is equivalent to Appellant's claimed authentication information, but Lewis does not teach or suggest that the registration information is generated using a key as claimed.

In addition, the Examiner continues to assert that Quick discloses Appellant's "claimed" encryption of the authentication information using a key. However, Appellant does not claim encrypting the authentication information. Instead, Appellant claims that the authentication information is generated using a first key. Appellant has repeatedly pointed out the correct claim language to the Examiner but the Examiner continues to misstate the language of the claim in order to support his use of Quick to reject the claims. When the claim language is read properly it is readily apparent that Quick does not disclose Appellant's element as actually claimed. Quick's authentication information includes a public key, but Quick does not teach or suggest that the public key is generated using a key as claimed. In fact, Quick uses the Diffie-Hellman algorithm to generate the public key and the Diffie-Hellman algorithm is not key-based.

The Examiner is further equating Lewis' mobile device with Appellant's claimed station and Lewis' access point with Appellant's claimed access point. However, Lewis only discloses the exchange of network encryption keys, not security preferences as defined by Appellant. Moreover, even if Lewis' encryption key could be properly interpreted as equivalent to Appellant's claimed security preference, Lewis does not teach or suggest that the mobile device receives a new encryption key from the access point in response to the mobile device requesting the key. Instead in Lewis, the access point sends the new network encryption key to the mobile device in response to the access point receiving the new network encryption from the key distribution server. In fact, the mobile device cannot request a new network encryption key because it has no way of learning that the key distribution server has changed the key.

Nonetheless, the Examiner asserts that Lewis' access point is equivalent to Appellants access point because Lewis discloses an encryption engine resides in the

access point, citing column 15, lines 25-34, Figure 1, block 54 (access point) and Figure 2, block 118 (encryption engine). However, the encryption engine 118 is described as only decrypting (col. 8, line 4-7) and encrypting messages (col. 15, lines 25-34). There is nothing in the cited sections of Lewis, or in Lewis as a whole, that suggest the encryption engine 118 sends a new network encryption key in response to a request from the mobile device. Thus, Lewis' access point cannot be properly equated with Appellant's claimed access point that does distribute a key in response to a request from a station.

Therefore, the combination of Lewis and Quick does not disclose each and every limitation claimed by Appellant for the station and access point in claim 1, and Appellant respectfully submits that claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, 40-42, 46-48 and 50-51 are patentable under 35 U.S.C. § 103(a) over the combination.

#### **B. Claims 42-45**

Claims 42-45 stand or fall together. Claim 42 is the representative claim for this § 103(a) rejection and claims a data structure.

The Examiner has rejected claim 42 using the same arguments he uses to reject claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, 40-42, 46-48 and 50-51. Appellant has repeatedly pointed out to the Examiner that neither Lewis nor Quick disclose any data structure, much less a data structure as claimed in claim 42. However, the Examiner continues to assert the same argument and has never acknowledged that Appellant is claiming a data structure or pointed to any disclosure in either reference that even suggests a data structure as claimed.

Because neither Lewis nor Quick teach or suggest the invention as claimed in claim 42, Appellant respectfully submits that claims 42-45 are patentable under 35 U.S.C. § 103(a) over the combination of Lewis and Quick.

#### **IV. Claims 4-8, 18, 23, 28, 33, 39, and 49 are patentable under 35 U.S.C. 103(a) over the combination of Lewis, Quick and Schneier.**

Claims 4-8, 18, 23, 28, 33, 39, and 49 stand or fall together. Claim 4 is the representative claim for this § 103(a) rejection and claims a particular security algorithm that is used to generate a key for the access point.

Schneier is directed toward various cryptographic processes. Because claim 4 depends from claim 1, Schneier must disclose the claimed elements that are missing from the combination of Lewis and Quick in order to have a proper *prima facie* case of obviousness. However, Schneier does not teach or suggest an access point that sends a security preference as claimed.

In the final Office Action dated February 17, 2006, the Examiner argued that the combination of Lewis, Quick and Schneier is proper. Appellant respectfully submits that Appellant has not challenged the validity of the combination during prosecution. Instead, Appellant has repeatedly pointed out that the Examiner has failed to state a proper *prima facie case of obviousness* because the combination does not teach each and every limitation of Appellant's claim 4. Since claim 4 includes all the limitations of claim 1, at least one of the references must disclose an access point that sends a security preference as claimed in claim 1. However, none of the references disclose an access point as claimed.

Therefore, the combination of Lewis, Quick and Schneier does not teach each and every limitation of Appellant's invention as claimed in claim 4, and Appellant respectfully submits that claims 4-8, 18, 23, 28, 33, 39, and 49 are patentable under 35 U.S.C. § 103(a) over the combination.

### **VIII. CONCLUSION**

Appellant respectfully submits that Appellant has overcome all the rejections of the pending claims. Therefore, Appellant respectfully requests the Board reverse the rejections of claims 1, 16, 21, 26, 31, 36, 42 and 46 under 35 U.S.C. § 112 and under 35 U.S.C. § 102 and the rejections of claims 1-51 under 35 U.S.C. § 103, and direct the Examiner to enter a Notice of Allowance for claims 1-51.

However, in the event the Board decides to remand the case to the Examiner for further prosecution, Appellant respectfully requests the Board instruct the Examiner to correct his misstatement of the language of the independent claims in subsequent Office Actions.

**Fee for Filing a Brief in Support of Appeal**

Enclosed is a check in the amount of \$500.00 to cover the fee for filing a brief in support of an appeal as required under 37 C.F.R. §§ 1.17(c) and 41.37(a).

**Deposit Account Authorization**

Authorization is hereby given to charge our Deposit Account No. 02-2666 for any charges that may be due. Furthermore, if an extension is required, then Appellant hereby requests such extension.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR  
& ZAFMAN LLP

Dated: July 17, 2006

  
Sheryl Sue Holloway  
Attorney for Appellant  
Registration No. 37,850

12400 Wilshire Boulevard  
Seventh Floor  
Los Angeles, CA 90025-1026  
(408) 720-8300 x309

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re Application of: ) Examiner: Tran, Tongoc  
 )  
 Vogel, J. Leslie III ) Art Unit: 2134  
 )  
 Application No. 09/659,864 ) Confirmation No.: 5866  
 )  
 Filed: September 12, 2000 )  
 )  
 For: USER CONTROL OF A )  
 SECURE WIRELESS )  
 COMPUTING NETWORK )  
 )

---

Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**CLAIMS APPENDIX FOR  
APPEAL BRIEF UNDER 37 C.F.R. § 41.37**

1. (Previously presented) A computerized method of establishing a secure wireless communications channel between an access point and a station, the channel being encrypted with a channel key, the method comprising:

sending, by the station to the access point through a setup connection, a request for a security preference for the access point;

sending, by the access point to the station through the setup connection, the security preference in response to the request when the access point can support the channel, wherein the security preference specifies one authentication protocol from a set of authentication protocols supported by the access point;

generating, by the station, authentication information using a first key when the security preference is shared key;

sending, by the station to the access point through the setup connection, the authentication information;

validating, by the access point, the station using the authentication information;

encrypting, by the access point, the channel key using a second key;

sending, by the access point to the station through the setup connection, the encrypted channel key;

decrypting, by the station, the channel key in response to receiving the encrypted channel key; and

sending, by the station to the access point, data encrypted with the channel key to establish the channel.

2. (Original) The method of claim 1, wherein the first and second keys are a self-distributed key.

3. (Original) The method of claim 2, further comprising:

generating, by the access point, the self-distributed key using a security algorithm when the security preference is shared key;

generating, by the station and sending to the access point, a first value using the security algorithm in response to receiving the security preference of shared key;

generating, by the access point, and sending to the station, a second value using the security algorithm and the first value in response to receiving the first value; and

calculating, by the station, the self-distributed key using the security algorithm and the second value in response to receiving the second value.

4. (Original) The method of claim 3, wherein the security algorithm is  $g^n \bmod p$  and further comprising:

obtaining, by the access point, integers  $x$ ,  $g$  and  $p$  to generate the self-distributed key  $k = g^x \bmod p$ ;

obtaining, by the station, the integers  $g$  and  $p$ , and an integer  $y$  to generate the first value  $Y = g^y \bmod p$ ;

generating, by the access point, the second value  $X = Y^x \bmod p$ ; and

setting, by the station,  $z$  equal to  $y^{-1}$  to calculate the self-distributed key  $k = X^z \bmod p$ .

5. (Original) The method of claim 4 wherein obtaining, by the station, the integers  $g$  and  $p$  comprises:

sending, by the access point to the station, the integers for  $g$  and  $p$ .

6. (Original) The method of claim 5, wherein the integers for  $g$  and  $p$  are sent to the station when the security preferences are sent by the access point.

7. (Original) The method of claim 5, wherein the integers for  $g$  and  $p$  are sent to the station when a user name and password for the station are registered with the access point.

8. (Original) The method of claim 4 further comprising:

publishing, by the access point, the integers  $g$  and  $p$  for a set of stations.

9. (Original) The method of claim 2 further comprising:

encrypting, by the station, a name and password with the first key to generate the authentication information; and

decrypting, by the access point, the name and password to validate the station.

10. (Original) The method of claim 2 further comprising:

sending, by the access point to the station, a challenge;

encrypting, by the station, the challenge with the first key to generate the authentication information;

encrypting, by the access point, the challenge with the first key; and

comparing, by the access point, the authentication information with the challenge encrypted by the access point with the first key to validate the station.

11. (Original) The method of claim 1, wherein the first key is a public key of a public-private key pair for the access point, and the second key is a public key of a public-private key pair for the station.

12. (Original) The method of claim 11 further comprising:

sending, by the access point to the station, the first key; and.

sending, by the station to the access point, the second key.

13. (Original) The method of claim 12, wherein the second key is sent to the access point when the request for the security preference is sent by the station.

14. (Original) The method of claim 12, wherein the first key is sent to the station when the security preference is sent by the access point.

15. (Original) The method of claim 1, wherein establishing the channel creates a standard wired equivalent privacy (WEP) network, and the station and the access point exchange messages conforming to a format required by the standard that defines a WEP network to establish the WEP network.

16. (Previously presented) A computerized method for connecting a station to a secure wireless network comprising:

sending a request for a security preference through a setup connection to an access point for the secure wireless network, wherein the security preference specifies one authentication protocol from a set of authentication protocols supported by the access point;

generating authentication information for the station when the station receives a security preference specifying shared key from the access point through the setup connection;

sending the authentication information to the access point through the setup connection;

decrypting a channel key in response to receiving an encrypted channel key from the access point through the setup connection; and

sending data encrypted with the channel key to the access point, wherein exchanging data encrypted with the channel key establishes a secure channel in the network.

17. (Original) The method of claim 16 further comprising:

generating a first value using a security algorithm in response to receiving the security preference specifying shared key from the access point;

calculating a self-distributed key using the security algorithm and a second value in response to receiving the second value from the access point; and

using the self-distributed key to generate the authentication information and to decrypt the encrypted channel key.

18. (Original) The method of claim 17, wherein the security algorithm is formulated as  $g^n$  mod  $p$  and further comprising:

obtaining integers for  $y$ ,  $g$  and  $p$  to generate the first value  $Y = g^y$  mod  $p$ ; and setting  $z$  equal to  $y^{-1}$  to calculate the self-distributed key  $k = X^z$  mod  $p$ .

19. (Original) The method of claim 16 further comprising:

using a first key to generate the authentication information; and  
using a second key to decrypt the encrypted channel key.

20. (Original) The method of claim 19, wherein the first key is a public key of a public-private key pair for the access point, and the second key is a private key of a public-private key pair for the station.

21. (Previously presented) A computerized method of securing a wireless network at an access point comprising:

sending a security preference through a setup connection in response to a request from a station, wherein the security preference specifies one authentication protocol from a set of authentication protocols supported by the access point;

validating the station in response to receiving authentication information from the station through the setup connection;

encrypting a channel key when the station is validated;

sending the encrypted channel key to the station through the setup connection;

and

sending data encrypted with the channel key to the station, wherein exchanging data encrypted with the channel key establishes a secure channel in the network.

22. (Original) The method of claim 21 further comprising:

generating a self-distributed key using a security algorithm when the security preference is shared key;

generating a second value using the security algorithm and a first value in response to receiving the first value from the station; and

sending the second value to the station.

23. (Original) The method of claim 22, wherein the security algorithm is formulated as  $g^n \text{ mod } p$  and further comprising:

obtaining integers  $x$ ,  $g$  and  $p$  to generate the self-distributed key  $k = g^x \text{ mod } p$ ; and generating the second value  $X = Y^x \text{ mod } p$ .

24. (Original) The method of claim 21 further comprising:

using a first key to evaluate the authentication information; and

using a second key to encrypt the encrypted channel key.

25. (Original) The method of claim 24, wherein the first key is a private key of a public-private key pair for the access point, and the second key is a public key of a public-private key pair for the station.

26. (Previously presented) A computer-readable medium having stored thereon executable instructions to cause a processor to perform a station method to connect to a secure wireless network, the instructions comprising:

sending a request for a security preference through a setup connection to an access point for the secure wireless network, wherein the security preference specifies one authentication protocol from a set of authentication protocols supported by the access point;

generating authentication information for the station when the station receives a security preference specifying shared key from the access point through the setup connection;

sending the authentication information to the access point through the setup connection;

decrypting a channel key in response to receiving an encrypted channel key from the access point through the setup connection; and

sending data encrypted with the channel key to the access point, wherein exchanging data encrypted with the channel key establishes a secure channel in the network.

27. (Original) The computer-readable medium of claim 26 having further instructions comprising:

generating a first value using a security algorithm in response to receiving the security preference specifying shared key from the access point;

calculating a self-distributed key using the security algorithm and a second value in response to receiving the second value from the access point; and

using the self-distributed key to generate the authentication information and to decrypt the encrypted channel key.

28. (Original) The computer-readable medium of claim 27, wherein the security algorithm is formulated as  $g^n \bmod p$  and having further instructions comprising:

obtaining integers  $y$ ,  $g$  and  $p$  to generate the first value  $Y = g^y \bmod p$ ; and  
setting  $z$  equal to  $y^{-1}$  to calculate the self-distributed key  $k = X^z \bmod p$ .

29. (Original) The computer-readable medium of claim 26 having further instructions comprising:

using a first key to generate the authentication information; and  
using a second key to decrypt the encrypted channel key.

30. (Original) The computer-readable medium of claim 29, wherein the first key is a public key of a public-private key pair for the access point, and the second key is a private key of a public-private key pair for the station.

31. (Previously presented) A computer-readable medium having stored thereon executable instruction to cause a processor to perform an access point method to secure a wireless network, the instructions comprising:

sending a security preference through a setup connection in response to a request from a station, wherein the security preference specifies one authentication protocol from a set of authentication protocols supported by the access point;

validating the station in response to receiving authentication information from the station through the setup connection;

encrypting a channel key when the station is validated;

sending the encrypted channel key to the station through the setup connection;  
and

sending data encrypted with the channel key to the station, wherein exchanging data encrypted with the channel key establishes a secure channel in the network.

32. (Original) The computer-readable medium of claim 31 having further instructions comprising:

generating a self-distributed key using a security algorithm when the security preference is shared key;

generating a second value using the security algorithm and a first value in response to receiving the first value from the station; and  
sending the second value to the station.

33. (Original) The computer-readable medium of claim 32, wherein the security algorithm is formulated as  $g^n \bmod p$  and having further instructions comprising:

obtaining integers  $x$ ,  $g$  and  $p$  to generate the self-distributed key  $k = g^x \bmod p$ ; and  
generating the second value  $X = Y^x \bmod p$ .

34. (Original) The computer-readable medium of claim 31 having further instructions comprising:

using a first key to evaluate the authentication information; and  
using a second key to encrypt the encrypted channel key.

35. (Original) The computer-readable medium of claim 34, wherein the first key is a private key of a public-private key pair for the access point, and the second key is a public key of a public-private key pair for the station.

36. (Previously presented) A secure wireless network comprising:

an access point operable for receiving a connection request from a station through a setup connection, for sending a security preference that specifies one authentication protocol from a set of authentication protocols supported by the access point, for validating authentication information sent by the station, and for connecting the station to the network through a channel secured with a shared channel key; and

a station operable for sending the connection request to the access point, and for generating the authentication information to send to the access point.

37. (Previously Presented) The secure wireless network of claim 36, wherein the access point is further operable for sending a security preference specifying shared key to the

station upon receiving the connection request, and the station is operable for sending the authentication information to the access point upon receiving a security preference specifying shared key.

38. (Original) The secure wireless network of claim 37, wherein the access point is further operable for encrypting the shared channel key using a self-distributed key for sending to the station and the station is further operable for decrypting the shared channel key upon receipt.

39. (Original) The secure wireless network of claim 38, wherein the station and the access point are further operable for calculating the self-distributed key by exchanging messages in accordance with the Hughes transmission protocol.

40. (Original) The secure wireless network of claim 36, wherein the station is further operable for using a first key to generate the authentication information and for using a second key to decrypt an encrypted shared channel key received from the access point, and the access point is further operable for using a third key to evaluate the authentication information and for using a fourth key to encrypt the shared channel key for sending to the station.

41. (Original) The secure wireless network of claim 40, wherein the first and third keys are public and private keys, respectively, for the access point, and the second and fourth keys are private and public keys, respectively, for the station.

42. (Previously presented) A computer-readable medium having stored thereon a message data structure for a secure wireless network comprising:

    a station address field containing data representing an identifier for a station that exchanges messages with an access point on the secure wireless network;

    a transaction sequence number field containing data representing a sequence number for a message exchanged between the station identified by the station address field and the access point;

an authentication algorithm field containing data representing an identifier for one authentication protocol from a set of authentication protocols supported by the access point, the one authentication protocol used by the access point to validate the station identified by the station address field based on a name and password for the station; and

a dependent information field containing data required to connect the station identified by the station address field to the secure wireless network.

43. (Original) The computer-readable medium of claim 42, wherein the data in the dependent information field represents key information for encrypting the name and password for the station identified by the station address field.

44. (Original) The computer-readable medium of claim 42, wherein the data in the dependent information field represents an encrypted name and password for the station identified by the station address field.

45. (Original) The computer-readable medium of claim 42, wherein the data in the dependent information field represents an encrypted channel key used to connect the station identified by the station address field to the secure wireless network.

46. (Previously presented) An apparatus comprising:

a means for accessing a wireless network, the means for accessing operable for receiving a connection request from a means for messaging through a setup connection, for sending a security preference that specifies one authentication protocol from a set of authentication protocols supported by the means for access, for validating authentication information sent by the means for messaging, and for connecting the means for messaging to the wireless network through a channel secured with a shared channel key; and

a means for messaging operable for sending the connection request to the means for accessing, and for generating the authentication information to send to the means for accessing.

47. (Previously presented) The apparatus of claim 46, wherein the means for accessing is further operable for sending a security preference specifying shared key to the means for messaging upon receiving the connection request, and the means for messaging is further operable for sending the authentication information to the means for accessing upon receiving a security preference specifying shared key.

48. (Previously presented) The apparatus of claim 47, wherein the means for accessing is further operable for encrypting the shared channel key using a self-distributed key for sending to the means for messaging and the means for messaging is further operable for decrypting the shared channel key upon receipt.

49. (Previously presented) The apparatus of claim 48, wherein the means for accessing and the means for messaging are further operable for calculating the self-distributed key by exchanging messages in accordance with the Hughes transmission protocol.

50. (Previously presented) The apparatus of claim 46, wherein the means for messaging is further operable for using a first key to generate the authentication information and for using a second key to decrypt an encrypted shared channel key received from the means for accessing, and the means for accessing is further operable for using a third key to evaluate the authentication information and for using a fourth key to encrypt the shared channel key for sending to the means for messaging.

51. (Previously presented) The apparatus of claim 50, wherein the first and third keys are public and private keys, respectively, for the means for accessing, and the second and fourth keys are private and public keys, respectively, for the means for messaging.

**EVIDENCE APPENDIX FOR  
APPEAL BRIEF UNDER 37 C.F.R. § 41.37**

Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)  
Specifications, *ANSI/IEEE Std. 802.11*, 1999 Edition, Part 11: pages i-ii, ix-xiv and 59-  
61.

**Information technology—  
Telecommunications and information  
exchange between systems—  
Local and metropolitan area networks—  
Specific requirements—**

**Part 11: Wireless LAN Medium Access  
Control (MAC) and Physical Layer  
(PHY) Specifications**

Sponsor

**LAN MAN Standards Committee  
of the  
IEEE Computer Society**

## ANSI/IEEE Std 802.11, 1999 Edition

IEEE Standards documents are developed within the Technical Committees of the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Board. Members of the committees serve voluntarily and without compensation. They are not necessarily members of the Institute. The standards developed within IEEE represent a consensus of the broad expertise on the subject within the Institute as well as those activities outside of IEEE that have expressed an interest in participating in the development of the standard.

Use of an IEEE Standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments.

**Interpretations:** Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of all concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason IEEE and the members of its technical committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration.

Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE Standards Board  
445 Hoes Lane  
P.O. Box 1331  
Piscataway, NJ 08855-1331  
USA

Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying all patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

The patent holder has, however, filed a statement of assurance that it will grant a license under these rights without compensation or under reasonable rates and nondiscriminatory, reasonable terms and conditions to all applicants desiring to obtain such a license. The IEEE makes no representation as to the reasonableness of rates and/or terms and conditions of the license agreement offered by the patent holder. Contact information may be obtained from the IEEE Standards Department.

Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; (978) 750-8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

## Contents

|   |    |
|---|----|
| 1. Overview.....  | 1  |
| 1.1 Scope.....  | 1  |
| 1.2 Purpose.....  | 1  |
| 2. Normative references.....                                    | 2  |
| 3. Definitions.....   | 3  |
| 4. Abbreviations and acronyms.....                              | 6  |
| 5. General description.....                                     | 9  |
| 5.1 General description of the architecture.....                | 9  |
| 5.1.1 How wireless LAN systems are different.....               | 9  |
| 5.2 Components of the IEEE 802.11 architecture.....             | 10 |
| 5.2.1 The independent BSS as an ad hoc network.....             | 10 |
| 5.2.2 Distribution system concepts.....                         | 11 |
| 5.2.3 Area concepts.....  | 12 |
| 5.2.4 Integration with wired LANs.....                          | 14 |
| 5.3 Logical service interfaces.....                             | 14 |
| 5.3.1 Station service (SS).....                                 | 15 |
| 5.3.2 Distribution system service (DSS).....                    | 15 |
| 5.3.3 Multiple logical address spaces.....                      | 16 |
| 5.4 Overview of the services.....                               | 17 |
| 5.4.1 Distribution of messages within a DS.....                 | 17 |
| 5.4.2 Services that support the distribution service.....       | 18 |
| 5.4.3 Access and confidentiality control services.....          | 19 |
| 5.5 Relationships between services.....                         | 21 |
| 5.6 Differences between ESS and IBSS LANs.....                  | 23 |
| 5.7 Message information contents that support the services..... | 24 |
| 5.7.1 Data.....   | 25 |
| 5.7.2 Association.....  | 25 |
| 5.7.3 Reassociation.....  | 25 |
| 5.7.4 Disassociation.....                                       | 26 |
| 5.7.5 Privacy.....  | 26 |
| 5.7.6 Authentication.....                                       | 26 |
| 5.7.7 Deauthentication.....                                     | 27 |
| 5.7.8 Reference model.....                                      | 27 |
| 6. MAC service definition.....                                  | 29 |
| 6.1 Overview of MAC services.....                               | 29 |
| 6.1.1 Asynchronous data service.....                            | 29 |
| 6.1.2 Security services.....                                    | 29 |
| 6.1.3 MSDU ordering.....  | 29 |
| 6.2 Detailed service specification.....                         | 30 |
| 6.2.1 MAC data services.....                                    | 30 |
| 7. Frame formats.....   | 34 |
| 7.1 MAC frame formats.....                                      | 34 |

|   |    |
|---|----|
| 7.1.1 Conventions .....                                     | 34 |
| 7.1.2 General frame format .....                            | 34 |
| 7.1.3 Frame fields .....                                    | 35 |
| 7.2 Format of individual frame types.....                   | 41 |
| 7.2.1 Control frames .....                                  | 41 |
| 7.2.2 Data frames .....                                     | 43 |
| 7.2.3 Management frames.....                                | 45 |
| 7.3 Management frame body components.....                   | 50 |
| 7.3.1 Fixed fields.....                                     | 50 |
| 7.3.2 Information elements .....                            | 55 |
| 8. Authentication and privacy .....                         | 59 |
| 8.1 Authentication services.....                            | 59 |
| 8.1.1 Open System authentication .....                      | 59 |
| 8.1.2 Shared Key authentication .....                       | 60 |
| 8.2 The Wired Equivalent Privacy (WEP) algorithm .....      | 61 |
| 8.2.1 Introduction.....                                     | 61 |
| 8.2.2 Properties of the WEP algorithm .....                 | 62 |
| 8.2.3 WEP theory of operation .....                         | 62 |
| 8.2.4 WEP algorithm specification .....                     | 64 |
| 8.2.5 WEP Frame Body expansion.....                         | 64 |
| 8.3 Security-Related MIB attributes .....                   | 65 |
| 8.3.1 Authentication-Related MIB attributes.....            | 65 |
| 8.3.2 Privacy-Related MIB attributes .....                  | 65 |
| 9. MAC sublayer functional description.....                 | 70 |
| 9.1 MAC architecture.....                                   | 70 |
| 9.1.1 Distributed coordination function (DCF).....          | 70 |
| 9.1.2 Point coordination function (PCF).....                | 70 |
| 9.1.3 Coexistence of DCF and PCF .....                      | 71 |
| 9.1.4 Fragmentation/defragmentation overview .....          | 71 |
| 9.1.5 MAC data service .....                                | 72 |
| 9.2 DCF .....   | 72 |
| 9.2.1 Carrier-sense mechanism .....                         | 73 |
| 9.2.2 MAC-Level acknowledgments .....                       | 73 |
| 9.2.3 Interframe space (IFS) .....                          | 74 |
| 9.2.4 Random backoff time.....                              | 75 |
| 9.2.5 DCF access procedure.....                             | 76 |
| 9.2.6 Directed MPDU transfer procedure .....                | 82 |
| 9.2.7 Broadcast and multicast MPDU transfer procedure ..... | 83 |
| 9.2.8 ACK procedure .....                                   | 83 |
| 9.2.9 Duplicate detection and recovery.....                 | 83 |
| 9.2.10 DCF timing relations.....                            | 84 |
| 9.3 PCF .....   | 86 |
| 9.3.1 CFP structure and timing .....                        | 87 |
| 9.3.2 PCF access procedure .....                            | 88 |
| 9.3.3 PCF transfer procedure .....                          | 89 |
| 9.3.4 Contention-Free polling list .....                    | 92 |
| 9.4 Fragmentation .....                                     | 93 |
| 9.5 Defragmentation .....                                   | 94 |
| 9.6 Multirate support.....                                  | 95 |
| 9.7 Frame exchange sequences .....                          | 95 |

|         |  |     |
|---------|--|-----|
| 9.8     | MSDU transmission restrictions .....                         | 97  |
| 10.     | Layer management .....                                       | 98  |
| 10.1    | Overview of management model .....                           | 98  |
| 10.2    | Generic management primitives .....                          | 98  |
| 10.3    | MLME SAP interface .....                                     | 100 |
| 10.3.1  | Power management .....                                       | 100 |
| 10.3.2  | Scan .....   | 101 |
| 10.3.3  | Synchronization .....  | 103 |
| 10.3.4  | Authenticate .....   | 105 |
| 10.3.5  | De-authenticate .....  | 107 |
| 10.3.6  | Associate .....  | 109 |
| 10.3.7  | Reassociate .....  | 111 |
| 10.3.8  | Disassociate .....   | 113 |
| 10.3.9  | Reset .....  | 114 |
| 10.3.10 | Start .....  | 116 |
| 10.4    | PLME SAP interface .....                                     | 118 |
| 10.4.1  | PLME-RESET.request .....                                     | 118 |
| 10.4.2  | PLME-CHARACTERISTICS.request .....                           | 118 |
| 10.4.3  | PLME-CHARACTERISTICS.confirm .....                           | 119 |
| 10.4.4  | PLME-DSSTESTMODE.request .....                               | 121 |
| 10.4.5  | PLME-DSSTESTOUTPUT.request .....                             | 122 |
| 11.     | MAC sublayer management entity .....                         | 123 |
| 11.1    | Synchronization .....  | 123 |
| 11.1.1  | Basic approach .....   | 123 |
| 11.1.2  | Maintaining synchronization .....                            | 123 |
| 11.1.3  | Acquiring synchronization, scanning .....                    | 125 |
| 11.1.4  | Adjusting STA timers .....                                   | 127 |
| 11.1.5  | Timing synchronization for frequency-hopping (FH) PHYs ..... | 128 |
| 11.2    | Power management .....                                       | 128 |
| 11.2.1  | Power management in an infrastructure network .....          | 128 |
| 11.2.2  | Power management in an IBSS .....                            | 133 |
| 11.3    | Association and reassociation .....                          | 136 |
| 11.3.1  | STA association procedures .....                             | 136 |
| 11.3.2  | AP association procedures .....                              | 136 |
| 11.3.3  | STA reassociation procedures .....                           | 136 |
| 11.3.4  | AP reassociation procedures .....                            | 137 |
| 11.4    | Management information base (MIB) definitions .....          | 137 |
| 12.     | Physical layer (PHY) service specification .....             | 138 |
| 12.1    | Scope .....  | 138 |
| 12.2    | PHY functions .....  | 138 |
| 12.3    | Detailed PHY service specifications .....                    | 138 |
| 12.3.1  | Scope and field of application .....                         | 138 |
| 12.3.2  | Overview of the service .....                                | 138 |
| 12.3.3  | Overview of interactions .....                               | 138 |
| 12.3.4  | Basic service and options .....                              | 139 |
| 12.3.5  | PHY-SAP detailed service specification .....                 | 140 |
| 13.     | PHY management .....   | 147 |

|     |  |     |
|-----|--|-----|
| 14. | Frequency-Hopping spread spectrum (FHSS) PHY specification for the 2.4 GHz Industrial, Scientific, and Medical (ISM) band..... | 148 |
|     | 14.1 Overview.....   | 148 |
|     | 14.1.1 Overview of FHSS PHY .....  | 148 |
|     | 14.1.2 FHSS PHY functions .....  | 148 |
|     | 14.1.3 Service specification method and notation .....   | 148 |
|     | 14.2 FHSS PHY-specific service parameter lists .....   | 149 |
|     | 14.2.1 Overview.....   | 149 |
|     | 14.2.2 TXVECTOR parameters.....  | 149 |
|     | 14.2.3 RXVECTOR parameters .....   | 150 |
|     | 14.3 FHSS PLCP sublayer.....   | 150 |
|     | 14.3.1 Overview.....   | 150 |
|     | 14.3.2 PLCP frame format.....  | 151 |
|     | 14.3.3 PLCP state machines.....  | 154 |
|     | 14.4 PLME SAP layer management .....   | 163 |
|     | 14.4.1 Overview.....   | 163 |
|     | 14.4.2 FH PHY specific MAC sublayer management entity (MLME) procedures.....   | 163 |
|     | 14.4.3 FH PHY layer management entity state machines .....   | 163 |
|     | 14.5 FHSS PMD sublayer services .....  | 166 |
|     | 14.5.1 Scope and field of application.....   | 166 |
|     | 14.5.2 Overview of services.....   | 166 |
|     | 14.5.3 Overview of interactions.....   | 166 |
|     | 14.5.4 Basic service and options.....  | 166 |
|     | 14.5.5 PMD_SAP detailed service specification .....  | 167 |
|     | 14.6 FHSS PMD sublayer, 1.0 Mbit/s .....   | 172 |
|     | 14.6.1 1 Mbit/s PMD operating specifications, general.....   | 172 |
|     | 14.6.2 Regulatory requirements .....   | 172 |
|     | 14.6.3 Operating frequency range.....  | 173 |
|     | 14.6.4 Number of operating channels .....  | 174 |
|     | 14.6.5 Operating channel center frequency .....  | 174 |
|     | 14.6.6 Occupied channel bandwidth.....   | 176 |
|     | 14.6.7 Minimum hop rate.....   | 176 |
|     | 14.6.8 Hop sequences .....   | 177 |
|     | 14.6.9 Unwanted emissions .....  | 179 |
|     | 14.6.10 Modulation .....   | 179 |
|     | 14.6.11 Channel data rate.....   | 180 |
|     | 14.6.12 Channel switching/settling time.....   | 180 |
|     | 14.6.13 Receive to transmit switch time .....  | 180 |
|     | 14.6.14 PMD transmit specifications .....  | 181 |
|     | 14.6.15 PMD receiver specifications .....  | 182 |
|     | 14.6.16 Operating temperature range.....   | 183 |
|     | 14.7 FHSS PMD sublayer, 2.0 Mbit/s .....   | 183 |
|     | 14.7.1 Overview.....   | 183 |
|     | 14.7.2 Four-Level GFSK modulation .....  | 184 |
|     | 14.7.3 Channel data rate.....  | 185 |
|     | 14.8 FHSS PHY management information base (MIB) .....  | 186 |
|     | 14.8.1 Overview.....   | 186 |
|     | 14.8.2 FH PHY attributes .....   | 187 |
|     | 14.9 FH PHY characteristics.....   | 194 |
| 15. | Direct sequence spread spectrum (DSSS) PHY specification for the 2.4 GHz band designated for ISM applications .....            | 195 |

|   |   |     |
|---|---|-----|
| 15.1  | Overview .....  | 195 |
| 15.1.1  | Scope .....   | 195 |
| 15.1.2  | DSSS PHY functions .....                                | 195 |
| 15.1.3  | Service specification method and notation .....         | 196 |
| 15.2  | DSSS PLCP sublayer .....                                | 196 |
| 15.2.1  | Overview .....  | 196 |
| 15.2.2  | PLCP frame format .....                                 | 196 |
| 15.2.3  | PLCP field definitions .....                            | 196 |
| 15.2.4  | PLCP/DSSS PHY data scrambler and descrambler .....      | 199 |
| 15.2.5  | PLCP data modulation and modulation rate change .....   | 199 |
| 15.2.6  | PLCP transmit procedure .....                           | 199 |
| 15.2.7  | PLCP receive procedure .....                            | 200 |
| 15.3  | DSSS physical layer management entity (PLME) .....      | 203 |
| 15.3.1  | PLME_SAP sublayer management primitives .....           | 203 |
| 15.3.2  | DSSS PHY MIB .....                                      | 204 |
| 15.3.3  | DS PHY characteristics .....                            | 205 |
| 15.4  | DSSS PMD sublayer .....                                 | 205 |
| 15.4.1  | Scope and field of application .....                    | 205 |
| 15.4.2  | Overview of service .....                               | 206 |
| 15.4.3  | Overview of interactions .....                          | 206 |
| 15.4.4  | Basic service and options .....                         | 206 |
| 15.4.5  | PMD_SAP detailed service specification .....            | 208 |
| 15.4.6  | PMD operating specifications, general .....             | 215 |
| 15.4.7  | PMD transmit specifications .....                       | 218 |
| 15.4.8  | PMD receiver specifications .....                       | 222 |
| 16.   | Infrared (IR) PHY specification .....                   | 224 |
| 16.1  | Overview .....  | 224 |
| 16.1.1  | Scope .....   | 225 |
| 16.1.2  | IR PHY functions .....                                  | 225 |
| 16.1.3  | Service specification method and notation .....         | 225 |
| 16.2  | IR PLCP sublayer .....                                  | 226 |
| 16.2.1  | Overview .....  | 226 |
| 16.2.2  | PLCP frame format .....                                 | 226 |
| 16.2.3  | PLCP modulation and rate change .....                   | 226 |
| 16.2.4  | PLCP field definitions .....                            | 227 |
| 16.2.5  | PLCP procedures .....                                   | 228 |
| 16.3  | IR PMD sublayer .....                                   | 230 |
| 16.3.1  | Overview .....  | 230 |
| 16.3.2  | PMD operating specifications, general .....             | 230 |
| 16.3.3  | PMD transmit specifications .....                       | 233 |
| 16.3.4  | PMD receiver specifications .....                       | 236 |
| 16.3.5  | Energy Detect, Carrier Sense, and CCA definitions ..... | 237 |
| 16.4  | PHY attributes .....                                    | 239 |
| Annex A (normative) Protocol Implementation Conformance Statement (PICS) proforma ..... |   | 241 |
| A.1   | Introduction .....                                      | 241 |
| A.2   | Abbreviations and special symbols .....                 | 241 |
| A.2.1   | Status symbols .....                                    | 241 |
| A.2.2   | General abbreviations .....                             | 241 |
| A.3   | Instructions for completing the PICS proforma .....     | 242 |
| A.3.1   | General structure of the PICS proforma .....            | 242 |

|  |     |
|--|-----|
| A.3.2 Additional information.....                                      | 242 |
| A.3.3 Exception information.....                                       | 243 |
| A.3.4 Conditional status.....  | 243 |
| A.4 PICS proforma—ISO/IEC 8802-11: 1999.....                           | 244 |
| A.4.1 Implementation identification.....                               | 244 |
| A.4.2 Protocol summary, ISO/IEC 8802-11: 1999.....                     | 244 |
| A.4.3 IUT configuration .....  | 245 |
| A.4.4 MAC protocol .....   | 245 |
| A.4.5 Frequency-Hopping PHY functions.....                             | 250 |
| A.4.6 Direct sequence PHY functions .....                              | 252 |
| A.4.7 Infrared baseband PHY functions.....                             | 255 |
| Annex B (informative) Hopping sequences.....                           | 259 |
| Annex C (normative) Formal description of MAC operation .....          | 272 |
| C.1 Introduction to the MAC formal description .....                   | 275 |
| C.2 Data type and operator definitions for the MAC state machines..... | 277 |
| C.3 State Machines for MAC stations.....                               | 324 |
| C.4 State machines for MAC access point .....                          | 400 |
| Annex D (normative) ASN.1 encoding of the MAC and PHY MIB.....         | 469 |
| Annex E (informative) Bibliography .....                               | 512 |
| E.1 General.....   | 512 |
| E.2 Specification and description language (SDL) documentation .....   | 512 |

## 8. Authentication and privacy

### 8.1 Authentication services

IEEE 802.11 defines two subtypes of authentication service: *Open System* and *Shared Key*. The subtype invoked is indicated in the body of authentication management frames. Thus authentication frames are self-identifying with respect to authentication algorithm. All management frames of subtype Authentication shall be unicast frames as authentication is performed between pairs of stations (i.e., multicast authentication is not allowed). Management frames of subtype Deauthentication are advisory, and may therefore be sent as group-addressed frames.

A mutual authentication relationship shall exist between two stations following a successful authentication exchange as described below. Authentication shall be used between stations and the AP in an infrastructure BSS. Authentication may be used between two STAs in an IBSS.

#### 8.1.1 Open System authentication

Open System authentication is the simplest of the available authentication algorithms. Essentially it is a null authentication algorithm. Any STA that requests authentication with this algorithm may become authenticated if dot11AuthenticationType at the recipient station is set to Open System authentication. Open System authentication is not required to be successful as a STA may decline to authenticate with any particular other STA. Open System authentication is the default authentication algorithm.

Open System authentication involves a two-step authentication transaction sequence. The first step in the sequence is the identity assertion and request for authentication. The second step in the sequence is the authentication result. If the result is “successful,” the STAs shall be mutually authenticated.

##### 8.1.1.1 Open System authentication (first frame)

- Message type: Management
- Message subtype: Authentication
- Information items:
  - Authentication Algorithm Identification = “Open System”
  - Station Identity Assertion (in SA field of header)
  - Authentication transaction sequence number = 1
  - Authentication algorithm dependent information (none)
- Direction of message: From authentication initiating STA to authenticating STA

##### 8.1.1.2 Open System authentication (final frame)

- Message type: Management
- Message subtype: Authentication
- Information items:
  - Authentication Algorithm Identification = “Open System”
  - Authentication transaction sequence number = 2
  - Authentication algorithm dependent information (none)
  - The result of the requested authentication as defined in 7.3.1.9
- Direction of message: From authenticating STA to initiating STA

If dot11AuthenticationType does not include the value “Open System,” the result code shall not take the value “successful.”

### 8.1.2 Shared Key authentication

Shared Key authentication supports authentication of STAs as either a member of those who know a shared secret key or a member of those who do not. IEEE 802.11 Shared Key authentication accomplishes this without the need to transmit the secret key in the clear; however, it does require the use of the WEP privacy mechanism. Therefore, this authentication scheme is only available if the WEP option is implemented. Additionally, the Shared Key authentication algorithm shall be implemented as one of the dot11AuthenticationAlgorithms at any STA where WEP is implemented.

The required secret, shared key is presumed to have been delivered to participating STAs via a secure channel that is independent of IEEE 802.11. This shared key is contained in a write-only MIB attribute via the MAC management path. The attribute is write-only so that the key value remains internal to the MAC.

During the Shared Key authentication exchange, both the challenge and the encrypted challenge are transmitted. This facilitates unauthorized discovery of the pseudorandom number (PRN) sequence for the key/IV pair used for the exchange. Implementations should therefore avoid using the same key/IV pair for subsequent frames.

A STA shall not initiate a Shared Key authentication exchange unless its dot11PrivacyOptionImplemented attribute is “true.”

In the following description, the STA initiating the authentication exchange is referred to as the *requester*, and the STA to which the initial frame in the exchange is addressed is referred to as the *responder*.

#### 8.1.2.1 Shared Key authentication (first frame)

- Message type: Management
- Message subtype: Authentication
- Information Items:
  - Station Identity Assertion (in SA field of header)
  - Authentication Algorithm Identification = “Shared Key”
  - Authentication transaction sequence number = 1
  - Authentication algorithm dependent information (none)
- Direction of message: From requester to responder

#### 8.1.2.2 Shared Key authentication (second frame)

Before sending the second frame in the Shared Key authentication sequence, the responder shall use WEP to generate a string of octets that shall be used as the authentication challenge text.

- Message type: Management
- Message subtype: Authentication
- Information Items:
  - Authentication Algorithm Identification = “Shared Key”
  - Authentication transaction sequence number = 2
  - Authentication algorithm dependent information = the authentication result.
  - The result of the requested authentication as defined in 7.3.1.9

If the status code is not “successful,” this shall be the last frame of the transaction sequence. If the status code is not “successful,” the content of the challenge text field is unspecified.

If the status code is “successful,” the following additional information items shall have valid contents:

Authentication algorithm dependent information = challenge text.

This field shall be of fixed length of 128 octets. The field shall be filled with octets generated by the WEP pseudo-random number generator (PRNG). The actual value of the challenge field is unimportant, but the value shall not be a single static value. The key and IV used when generating the challenge text are unspecified because this key/IV value does not have to be shared and does not affect interoperability.

- Direction of message: From responder to requester

#### **8.1.2.3 Shared Key authentication (third frame)**

The requester shall copy the challenge text from the second frame into the third frame. The third frame shall be transmitted after encryption by WEP, as defined in 8.2.3, using the shared secret key.

- Message type: Management
- Message subtype: Authentication
- Information Items:
  - Authentication Algorithm Identification = “Shared Key”
  - Authentication transaction sequence number = 3
  - Authentication algorithm dependent information = challenge text from sequence two frame
- Direction of message: From requester to responder

This frame shall be encrypted as described below.

#### **8.1.2.4 Shared Key authentication (final frame)**

The responder shall attempt to decrypt the contents of the third frame in the authentication sequence as described below. If the WEP ICV check is successful, the responder shall then compare the decrypted contents of the Challenge Text field to the challenge text that was sent in Frame 2 of the sequence. If they are the same, then the responder shall respond with a successful status code in Frame 4 of the sequence. If the WEP ICV check fails, the responder shall respond with an unsuccessful status code in Frame 4 of the sequence as described below.

- Message type: Management
- Message subtype: Authentication
- Information Items:
  - Authentication Algorithm Identification = “Shared Key”
  - Authentication transaction sequence number = 4
  - Authentication algorithm dependent information = the authentication result
    - The result of the requested authentication.
    - This is a fixed length item with values “successful” and “unsuccessful.”
- Direction of message: From responder to requester

### **8.2 The Wired Equivalent Privacy (WEP) algorithm**

#### **8.2.1 Introduction**

Eavesdropping is a familiar problem to users of other types of wireless technology. IEEE 802.11 specifies a wired LAN equivalent data confidentiality algorithm. *Wired equivalent privacy* is defined as protecting authorized users of a wireless LAN from casual eavesdropping. This service is intended to provide functionality for the wireless LAN equivalent to that provided by the physical security attributes inherent to a wired medium.

Data confidentiality depends on an external key management service to distribute data enciphering/deciphering keys. The IEEE 802.11 standards committee specifically recommends against running an IEEE 802.11

**RELATED PROCEEDINGS APPENDIX FOR  
APPEAL BRIEF UNDER 37 C.F.R. § 41.37**

NONE



JUL 21 2006

TRANSMITTALPATENT

Application No.: 09/659,864  
Filing Date: September 12, 2000  
First Named Inventor J. Leslie Vogel, III  
Examiner's Name: Tongoc Tran  
Art Unit: 2134  
Attorney Docket No.: 004860.P2436

An Amendment After Final Action (37 CFR 1.116) is attached and applicant(s) request expedited action.

Charge any fee not covered by any check submitted to Deposit Account No. 02-2666.  
 Applicant(s) hereby request and authorize the U.S. Patent and Trademark Office to (1) treat any concurrent or future reply that requires a petition for extension of time as incorporating a petition for extension of time for the appropriate length of time and (2) charge all required fees, including extension of time fees and fees under 37 CFR 1.16 and 1.17, for any concurrent or future reply to Deposit Account No. 02-2666.  
Applicant(s) claim small entity status (37 CFR 1.27).

ATTACHMENTS

Preliminary Amendment  
Amendment/Response with respect to Office Action  
Amendment/Response After Final Action (37 CFR 1.116) (reminder: consider filing a Notice of Appeal)  
Notice of Appeal  
RCE (Request for Continued Examination)  
Supplemental Declaration  
Terminal Disclaimer (reminder: if executed by an attorney, the attorney must be properly of record)  
Information Disclosure Statement (IDS)  
Copies of IDS citations  
Petition for Extension of Time  
 Fee Transmittal Document (that includes a fee calculation based on the type and number of claims)  
Cross-Reference to Related Application(s)  
Certified Copy of Priority Document  
 Other: Appeal Brief  
 Other: Exhibit A-13 pages, Exhibit B-12 pages, Exhibit C- 1 page  
 Check(s)  
 Postcard (Return Receipt)

SUBMITTED BY:

BLAKELY SOKOLOFF TAYLOR &amp; ZAFMAN LLP

TYPED OR PRINTED NAME: Sheryl Sue Holloway

SIGNATURE:

REG. NO.: 37,850

DATE: July 17, 2006

ADDRESS: 12400 Wilshire Boulevard, Seventh Floor

Los Angeles, California 90025

TELEPHONE NO.: (408) 720-8300

CERTIFICATE OF MAILING BY FIRST CLASS MAIL (if applicable)

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria Virginia 22313-1450  
on 7.17.06

Date of Deposit

Carla Anysia Nascimento

Name of Person Mailing Correspondence

Signature

7.17.06

Date

Express Mail Label No. (if applicable):

(10/14/03)

Send to: COMMISSIONER FOR PATENTS, P.O. Box 1450, Alexandria, Virginia 22313-1450



AF  
JW

## FEE TRANSMITTAL FOR FY 2006

Effective on 12/08/2004. Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

**TOTAL AMOUNT OF PAYMENT (\$)** 500.00

Complete if Known:

Application No. 09/659,864  
 Filing Date September 12, 2000  
 First Named Inventor J. Leslie Vogel, III  
 Examiner Name Tongoc Tran  
 Art Unit 2134  
 Attorney Docket No. 004860.P2436

Applicant claims small entity status. See 37 CFR 1.27.

### METHOD OF PAYMENT (check all that apply)

Check  Credit Card  Money Order  None  Other (please identify)

#### Deposit Account

Deposit Account Number : 02-2666

Deposit Account Name: \_\_\_\_\_

The Director is Authorized to do the following with respect to the above-identified Deposit Account:

Charge fee(s) indicated below.

Charge any additional fee(s) or underpayment of fee(s) during the pendency of this application.

Charge fee(s) indicated below except for the filing fee

Credit any overpayments.

Any concurrent or future reply that requires a petition for extension of time should be treated as incorporating an appropriate petition for extension of time and all required fees should be charged.

Warning: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

### FEE CALCULATION

#### 1. BASIC FILING, SEARCH, AND EXAMINATION FEES

| Large Entity |      | Small Entity |      | Fee Description                    | <u>Fees Paid (\$)</u> |
|--------------|------|--------------|------|------------------------------------|-----------------------|
| Fee          | Fee  | Fee          | Fee  |                                    |                       |
| Code         | (\$) | Code         | (\$) | Utility application filing fee     | _____                 |
| 1011         | 300  | 2011         | 150  |                                    |                       |
| 1111         | 500  | 2111         | 250  | Utility search fee                 | 1,000/500             |
| 1311         | 200  | 2311         | 100  | Utility examination fee            | _____                 |
|              |      |              |      |                                    |                       |
| 1012         | 200  | 2012         | 100  | Design application filing fee      | _____                 |
| 1112         | 100  | 2112         | 50   | Design search fee                  | 430/215               |
| 1312         | 130  | 2312         | 65   | Design examination fee             | _____                 |
|              |      |              |      |                                    |                       |
| 1013         | 200  | 2013         | 100  | Plant filing fee                   | _____                 |
| 1113         | 300  | 2113         | 150  | Plant search fee                   | 660/330               |
| 1313         | 160  | 2313         | 80   | Plant examination fee              | _____                 |
|              |      |              |      |                                    |                       |
| 1004         | 300  | 2004         | 150  | Reissue filing fee                 | _____                 |
| 1114         | 500  | 2114         | 250  | Reissue search fee                 | 1,400/700             |
| 1314         | 600  | 2314         | 300  | Reissue examination fee            | _____                 |
|              |      |              |      |                                    |                       |
| 1005         | 200  | 2005         | 100  | Provisional application filing fee | _____                 |

**SUBTOTAL (1) \$ 0.00**

## **2. EXCESS CLAIM FEES**

|   | <u>Extra Claims</u>       | <u>Fee from<br/>below</u> | <u>Fees Paid (\$)</u> |
|---|---------------------------|---------------------------|-----------------------|
| <b>Total Claims</b> _____   | <b>- 20 or HP =</b> _____ | X \$50.00                 | = _____               |
| HP = highest number of total claims paid for, if greater than 20      |                           |                           |                       |
| <b>Independent Claims</b> _____                                       | <b>- 3 or HP =</b> _____  | X \$200.00                | = _____               |
| HP = highest number of independent claims paid for, if greater than 3 |                           |                           |                       |
| <b>Multiple Dependent Claims</b>                                      |                           | _____                     | = _____               |

### **3. APPLICATION SIZE FEE**

If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

| <u>Total Sheets</u> | <u>Extra Sheets</u> | <u>Number of each add'l<br/>50 or fraction thereof</u> | <u>Fee from<br/>below</u> | <u>Fees paid (\$)</u> |
|---------------------|---------------------|--|---------------------------|-----------------------|
| – 100 =             | / 50 =              | (round up to whole number)                             | X                         | \$250.00              |

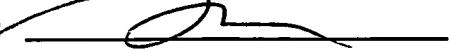
| <u>Large Entity</u> |          | <u>Small Entity</u> |          | <u>Fee Description:</u> Application size fee for each additional group of 50 sheets beyond initial 100 sheets (count spec & drawings except sequences & program listings): |
|---------------------|----------|---------------------|----------|--|
| Fee Code            | Fee (\$) | Fee Code            | Fee (\$) |  |
| 1081                | 250      | 2081                | 125      | Utility  |
| 1082                | 250      | 2082                | 125      | Design   |
| 1083                | 250      | 2083                | 125      | Plant  |
| 1084                | 250      | 2084                | 125      | Reissue  |

**SUBTOTAL (3) \$ 0.00**

**FEE CALCULATION (continued)****4. OTHER FEE(S)**

| <u>Large Entity</u>       | <u>Small Entity</u> | <u>Fee Description</u> | <u>Fees Paid (\$)</u>   |
|---------------------------|---------------------|------------------------|---|
| Fee Code                  | Fee Code            | Fee                    |   |
| 1051                      | 130                 | 2051                   | 65 Surcharge - late filing fee or oath  |
| 1052                      | 50                  | 2052                   | 25 Surcharge - late provisional filing fee or cover sheet                     |
| 1053                      | 130                 | 1053                   | 130 Non-English specification   |
| 1812                      | 2,520               | 1812                   | 2,520 For filing a request for ex parte reexamination                         |
| 1813                      | 8,800               | 1813                   | 8,800 Request for inter parties reexamination                                 |
| 1804                      | 920*                | 1804                   | 920* Requesting publication of SIR prior to Examiner action                   |
| 1805                      | 1,840*              | 1805                   | 1,840* Requesting publication of SIR after Examiner action                    |
| 1251                      | 120                 | 2251                   | 60 Extension for reply within first month                                     |
| 1252                      | 450                 | 2252                   | 225 Extension for reply within second month                                   |
| 1253                      | 1,020               | 2253                   | 510 Extension for reply within third month                                    |
| 1254                      | 1,590               | 2254                   | 795 Extension for reply within fourth month                                   |
| 1255                      | 2,160               | 2255                   | 1,080 Extension for reply within fifth month                                  |
| 1401                      | 500                 | 2401                   | 250 Notice of Appeal  |
| 1402                      | 500                 | 2402                   | 250 Filing a brief in support of an appeal                                    |
| 1403                      | 1,000               | 2403                   | 500 Request for oral hearing  |
| 1451                      | 1,510               | 1451                   | 1,510 Petition to institute a public use proceeding                           |
| 1452                      | 500                 | 2452                   | 250 Petition to revive – unavoidable  |
| 1453                      | 1,500               | 2453                   | 750 Petition to revive - unintentional  |
| 1501                      | 1,400               | 2501                   | 700 Utility issue fee (or reissue)  |
| 1502                      | 800                 | 2502                   | 400 Design issue fee  |
| 1503                      | 1100                | 2503                   | 550 Plant issue fee   |
| 1462                      | 400                 | 1462                   | 400 Petitions to the Commissioner (CFR 1.17(f) Group I)                       |
| 1463                      | 200                 | 1463                   | 200 Petitions to the Commissioner (CFR 1.17(g) Group II)                      |
| 1464                      | 130                 | 1464                   | 130 Petitions to the Commissioner (CFR 1.17(h) Group III)                     |
| 1807                      | 50                  | 1807                   | 50 Processing fee under 37 CFR 1.17(q)  |
| 1806                      | 180                 | 1806                   | 180 Submission of Information Disclosure Stmt                                 |
| 8021                      | 40                  | 8021                   | 40 Recording each patent assignment per property (times number of properties) |
| 1809                      | 790                 | 2809                   | 395 For filing a submission after final rejection (see 37 CFR 1.129(a))       |
| 1814                      | 130                 | 2814                   | 65 Statutory Disclaimer   |
| 1810                      | 790                 | 2810                   | 395 For each additional invention to be examined (see 37 CFR 1.129(b))        |
| 1801                      | 790                 | 2801                   | 395 Request for Continued Examination (RCE)                                   |
| 1802                      | 900                 | 1802                   | 900 Request for expedited examination of a design application                 |
| 1504                      | 300                 | 1504                   | 300 Publication fee for early, voluntary, or normal pub.                      |
| 1505                      | 300                 | 1505                   | 300 Publication fee for republication   |
| 1803                      | 130                 | 1803                   | 130 Request for voluntary publication or republication                        |
| 1808                      | 130                 | 1808                   | 130 Processing fee under 37 CFR 1.17(i) (except provisionals)                 |
| 1454                      | 1,370               | 1454                   | 1,370 Acceptance of unintentionally delayed claim for priority                |
| Other fee (specify) _____ |                     |                        |   |
| Other fee (specify) _____ |                     |                        |   |
| SUBTOTAL (4) \$           |                     |                        | <u>500.00</u>   |

\*Reduced by Basic Filing Fee Paid

**SUBMITTED BY:**Typed or Printed Name: Sheryl Sue HollowaySignature: Date: July 17, 2006Reg. Number: 37,850Telephone Number: 408-720-8300

Send to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450